The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/09/2019

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iCloud, iTunes, and macOS Catalina. The most severe of these vulnerabilities could allow for arbitrary code execution.

- iCloud is a cloud storage service.
- iTunes is a media player, media library, online radio broadcaster, and mobile device management application developed by Apple.
- macOS Catalina is a desktop operating system for Macintosh computers.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- iCloud for Windows 7 prior to 7.14
- iCloud for Windows 10 prior to 10.7
- iTunes for Windows prior to 12.10.1
- macOS Catalina 10.15

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in iCloud, iTunes, and macOS Catalina. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A buffer overflow was addressed with improved bounds checking. (CVE-2019-8745)
- A logic issue was addressed with improved restrictions. (CVE-2019-8755)
- A logic issue was addressed with improved state management. (CVE-2019-8625, CVE-2019-8719)
- A memory corruption issues were addressed with improved memory handling. (CVE-2019-8701, CVE-2019-8717, CVE-2019-8748, CVE-2019-8758)
- A memory corruption issues were addressed with improved memory handling. (CVE-2019-8707, CVE-2019-8720, CVE-2019-8726, CVE-2019-8733, CVE-2019-8735, CVE-2019-8763)
- A memory corruption issue was addressed with improved state management. (CVE-2019-8781)
- A memory corruption issue was addressed with improved validation. (CVE-2019-8705)
- An issue existed in the drawing of web page elements. The issue was addressed with improved logic. (CVE-2019-8769)
- An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt. (CVE-2019-8772)
- A race condition existed when reading and writing user preferences. This was addressed with improved state handling. (CVE-2019-8757)
- Multiple issues were addressed by updating to PHP version 7.3.8. (CVE-2019-11041, CVE-2019-11042)
- “Clear History and Website Data” did not clear the history. The issue was addressed with improved data deletion. (CVE-2019-8768)
- The contents of locked notes sometimes appeared in search results. This issue was addressed with improved data cleanup. (CVE-2019-8730)
- The issue was addressed with improved permissions logic. (CVE-2019-8770)

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT210634
https://support.apple.com/en-us/HT210635
https://support.apple.com/en-us/HT210636
https://support.apple.com/en-us/HT210637

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8625
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8701
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8705
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8707
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8717
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8719
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8720
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8726
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8730
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8733
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8735
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8755
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8757
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8758
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8763
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8768
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8769
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8770
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8772
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8781
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11041
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11042

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov